

NONCOMMUTATIVE GRÖBNER BASES OVER RINGS

ANDRÉ MIALEBAMA BOUESSO AND DJIBY SOW

Département de Mathématiques et Informatique
Laboratoire d'Algèbre, de Cryptologie, de Géométrie Algébrique et Applications
Université Cheikh Anta Diop
BP 5005 Dakar Fann, Sénégal
E-mails : miales2001@yahoo.fr, sowdjibab@yahoo.fr

ABSTRACT. In this work, it is proposed a method for computing Noncommutative Gröbner bases over a valuation noetherian ring. We have generalized the fundamental theorem on normal forms over an arbitrary ring. The classical method of dynamical commutative Gröbner bases is generalized for Buchberger's algorithm over $R = \mathcal{V}\langle x_1, \dots, x_m \rangle$ a free associative algebra with non-commuting variables, where $\mathcal{V} = \mathbb{Z}/n\mathbb{Z}$ or $\mathcal{V} = \mathbb{Z}$.

The process proposed, generalizes previous known technics for the computation of Commutative Gröbner bases over a valuation noetherian ring and/or Noncommutative Gröbner bases over a field.
Keywords: Noncommutative Gröbner bases, Commutative Gröbner bases, valuation noetherian ring, Buchberger algorithm, Dikson lemma, Termination theorem

CONTENTS

Introduction	1
1. Preliminaries	2
2. Noncommutative Gröbner bases over a commutative ring \mathcal{V}	3
2.1. Noncommutative Gröbner basis	3
2.2. Division algorithm	5
2.3. Reduced noncommutative Gröbner basis	6
3. Noncommutative Gröbner bases over noetherian valuation ring	7
4. Noncommutative Gröbner bases over $R = \frac{\mathbb{Z}}{n\mathbb{Z}}\langle x_1, \dots, x_m \rangle$	11
5. Noncommutative Gröbner bases over the integers	12
5.1. Special and Dynamical noncommutative Gröbner bases	12
5.2. Buchberger's algorithm for Dynamical noncommutative Gröbner basis	13
6. Acknowledgment	14
References	14

INTRODUCTION

Gröbner Bases is an algebraic technic that provides algorithmic solutions to a variety of problems in Algebra and Algebraic Geometry. Noncommutative and Commutative Gröbner bases over a field provides many applications in computable algebras such as coding theory and cryptography.

Many authors have introduced and/or generalized Commutative Gröbner bases in different ways over fields or rings with zeros divisors (and non invertible elements more generally): see [3], [4], [5], [6], [8], [15], [16], and [26].

Noncommutative Gröbner bases was also studied and developed by many authors (see: [7], [10], [11], [19] and [20]).

Most of concepts on noncommutative Gröbner bases over a field is analogous to the commutative case over a field. Nevertheless, some of the important differences are:

- most ideals of noncommutative algebras do not have finite Gröbner bases,
- it is possible to find a noncommutative Gröbner bases nonempty through a single polynomial.
- in some cases, the computation of the overlap relation (S-polynomial) of two polynomials in Buchberger algorithm, is not possible.

Throughout this paper, we propose a method for computing Noncommutative Gröbner bases over a valuation noetherian ring $\mathbb{Z}/n\mathbb{Z}$ and \mathbb{Z} . Our process generalizes previous known technics for the computation of Buchberger's algorithm in Commutative Gröbner bases over a valuation noetherian ring or in Commutative dynamical Gröbner bases over a principal ideal ring [25], [26] and in Noncommutative Gröbner bases over a field [11],[10], [19], [20]. In this paper, we work with $R = \mathcal{V}\langle x_1, \dots, x_m \rangle$ a free associative algebra with non-commuting variables over a ring \mathcal{V} . Although most of the results that we present here hold for a wider class of noncommutative algebras.

This paper is structured as follows:

Section 1: Preliminaries: we adapt to ring, the classical notions needed for Buchberger's algorithm in R .

Section 2: We introduce Noncommutative Gröbner bases and Reduced Gröbner bases and we give also the fundamental theorem on normal forms over R .

Section 3: We give the division algorithm and Buchberger's algorithm for Noncommutative Gröbner bases over a valuation noetherian ring \mathcal{V} .

Section 4: We have generalized Noncommutative Gröbner bases over $\mathcal{V} = \frac{\mathbb{Z}}{n\mathbb{Z}}$.

Section 5: We adapt dynamical commutative Gröbner bases to Noncommutative Gröbner bases over the integers $\mathcal{V} = n\mathbb{Z}$.

1. PRELIMINARIES

In this section, we give some notions and notations that we will use in the sequel.

Let \mathcal{V} be a commutative ring. \mathcal{V} is said to be a valuation ring if for all $a, b \in \mathcal{V}$, a divides b or b divides a .

A finite set of symbol is called alphabet. A finite sequence of elements of an alphabet Σ is called a word. By a monomial, we mean a finite noncommutative word in the alphabet $\{x_1, \dots, x_m\}$. We use the letter \mathbb{M} to denote the set of monomials. We define the multiplication in the set \mathbb{M} by concatenation. Let $p \in \mathbb{M}$, we denote by $Lth(p)$ the length of p i.e the number of letter of the word p . Note that $Lth(w) = 0$ if w is an empty word.

Let $R = \mathcal{V}\langle x_1, \dots, x_n \rangle$ be the free associative algebra with non-commuting variables defined over a ring \mathcal{V} , then $f \in R \Leftrightarrow f = \sum_{\alpha} a_{\alpha} p_{\alpha}$ as a finite sum, where $p_{\alpha} \in \mathbb{M}$ and $a_{\alpha} \in \mathcal{V}$ with $p_{\alpha} \neq p'_{\alpha}$ if $\alpha \neq \alpha'$. By a term t , we mean $t = ap$ where $a \in \mathcal{V}$ and $p \in \mathbb{M}$. We use the letter \mathbb{T} to denote the set of terms. We define the multiplication in the set \mathbb{T} as follows: if $t = ap$, $t' = a'p'$, with $a, a' \in \mathcal{V}$ and $p, p' \in \mathbb{M}$, then $tt' = aa'pp'$ where pp' is a concatenation of p and p' (p and p' do not commute). Let $t \in \mathbb{T}$. if $t = ap$ where $a \in \mathcal{V}$ and $p \in \mathbb{M}$, then $Lth(t) = Lth(p)$.

A subset I of R is said to be a two-sided ideal of R if:

- $g_1 - g_2 \in I$ for all $g_1, g_2 \in I$
- $f.g.h \in I$ for all $g \in I$ and all $f, h \in R$.

Let $D \subset R$, we denote by $\langle D \rangle = \{ \sum f.g.h/f, h \in R, g \in D \}$ the ideal generated by D and we denote also by $\langle\langle D \rangle\rangle = \{ \sum_i \alpha_i.g_i/\alpha_i \in \mathcal{V}, g_i \in D \}$ the \mathcal{V} -submodule of R generating by D .

- An ideal $I \subset R$ is said to be a term-ideal if it is generated by elements in \mathbb{T} of the form ap with $a = 1$ or $a \in \mathcal{V} \setminus \mathcal{V}^*$ and $p \in \mathbb{M}$ (where \mathcal{V}^* is the group of invertible elements of \mathcal{V}).

Let p and q be two monomials of \mathbb{M} . We say that p divides q if there exists two monomials m and m' of \mathbb{M} such that $q = m.p.m'$. Let $p \in \mathbb{M}$, we say that p occurs in $f \in \mathcal{V}\langle x_1, \dots, x_m \rangle$ if the

coefficient of p in f is not zero. Let $t = ap$ and $t' = a'p'$ two terms of \mathbb{T} . We say that t divides t' , if a divides a' in \mathcal{V} and p divides p' in \mathbb{M} .

The set \mathbb{M} of monomials is a monoïd with the concatenation as monoïd law.

A well-order $<$ on \mathbb{M} is said to be admissible, if it satisfies the following conditions: for all $p, q, r, s \in \mathbb{M}$, non empty :

- if $p < q$ then $pr < qr$
- if $p < q$ then $sp < sq$ and
- if $p = qr$ then $p > q$ and $p > r$.

In other words, $<$ is an admissible order if it is a well-order which is compatible with the monoïd structure. Note that the admissible order generalizes the notion of monomial order for the commutative case.

Let p and q be two monomials in the finite alphabet $\{x_1, x_2, \dots, x_n\}$. Considering that $x_1 < x_2 < \dots < x_n$, the left graded lexicographic order (grlex) is defined as follows: $p <_{grlex} q$ for the left graded lexicographic order if:

- $Lth(p) < Lth(q)$ or
- if $Lth(p) = Lth(q)$, we find the biggest common left subword m such that $p = m.w_1$ and $p_2 = m.w_2$ where $w_1 < w_2$ i.e the first symbol x_i for w_1 is smaller than the first symbol x_j for w_2 i.e $x_i < x_j$.

The left graded lexicographic order is an admissible order.

Throughout this paper we assume that $<$ is an admissible order.

- Let $q \in \mathbb{M}$, we say that q is the leading monomial of f and we note $q = LM(f)$ if q occurs in $f \in \mathcal{V}\langle x_1, \dots, x_m \rangle$ and $p < q$ for all monomials p occurring in f .
- The coefficient of the leading monomial of f is denoted $LC(f)$: it called the leading coefficient in f . The term $LT(f) = LC(f)LM(f)$ is the leading term of f .
- Let $E \subset R$, be a non empty set; and we define the following sets:
 - $LM(E) := \{LM(f)/f \in E \setminus \{0\}\}$.
 - $LT(E) := \{LT(g)/g \in E \setminus \{0\}\}$.
 - $NonLM(E) := \mathbb{M} \setminus LM(E)$.
 - $NonLT(E) := \mathbb{T} \setminus LT(E)$.

2. NONCOMMUTATIVE GRÖBNER BASES OVER A COMMUTATIVE RING \mathcal{V}

In this section $R = \mathcal{V}\langle X_1, \dots, X_n \rangle$ is a free associative algebra with noncommutative variables over a commutative ring \mathcal{V} and $<$ an admissible order on the set of all monomials \mathbb{M} .

2.1. Noncommutative Gröbner basis.

- Lemma 2.1.** (1) Let I be a term-ideal of R . Then a term $b_\beta.q_\beta \in I$ if and only if there exists $\alpha_0 p_{\alpha_0}$ in the set of generators of I which divides $b_\beta.q_\beta$.
- (2) Let $K = \langle \langle a_\alpha p_\alpha / p_\alpha \in \mathbb{M}, \alpha \in \Omega \subseteq \mathbb{N}^n \rangle \rangle$ be a \mathcal{V} -submodule of R . A term $b_\beta.q_\beta \in K$ if and only if there exists $\alpha_0 \in \Omega$ such that $p_{\alpha_0} = q_\beta$ and a_{α_0} divides b_β .

Proof Obvious □

Definition 2.2. A subset $G \subset I$ (where I is an ideal of R) is said to be a (two.sided) noncommutative Gröbner basis for I with respect to $<$ if

$$\langle LT(G) \rangle = \langle LT(I) \rangle$$

How to construct a noncommutative Gröbner basis? The classical method is Buchberger's algorithm. We will see how to design Buchberger's algorithm over a valuation nöetherian ring (section 3) and over a principal ideal ring (section 4).

In the following, we generalize the fundamental theorem on normal forms over R .

Theorem 2.3. *Let I be a \mathcal{V} -submodule of R , then, as a \mathcal{V} -module, we have:*

$$R = I \oplus \langle\langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle\rangle \oplus \langle\langle NonLM(I) \rangle\rangle,$$

where $\langle\langle X \rangle\rangle$ is the \mathcal{V} -submodule of R generated by $X \subseteq R$.

NB: If $LC(f)$ is invertible for every $f \in I$, then $\mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) = \emptyset$, thus, over a field $R = I \oplus \langle\langle NonLM(I) \rangle\rangle$ and we retrieve the classical known result for normal forms.

Proof

Put $A = I$, $B = \langle\langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle\rangle$ and $C = \langle\langle NonLM(I) \rangle\rangle$. First observe that $A \cap B = B \cap C = A \cap C = 0$; know, we are going to prove that $A \cap (B \oplus C) = 0$, $B \cap (A \oplus C) = 0$ and $C \cap (A \oplus B) = 0$.

(1) Let us prove that $A \cap (B \oplus C) = 0$, $B \cap (A \oplus C) = 0$ and $C \cap (A \oplus B) = 0$.

(a) Suppose that $f \in A \cap (B \oplus C)$ and $f \neq 0$. We have $f \in A = I \Rightarrow LM(f) \in LM(I)$ and $LT(f) \in LT(I)$ (*). On the other hand, we have: $f \in B \oplus C \Rightarrow LT(f) \in \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I)$ or $LM(f) \in NonLM(I)$. Thus, using (*) we have $LT(f) \in LT(I) \cap [\mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I)] = \emptyset$ or $LM(f) \in LM(I) \cap NonLM(I) = \emptyset$ which is impossible. Hence $A \cap (B \oplus C) = 0$.

(b) Suppose that $f \in B \cap (A \oplus C)$ and $f \neq 0$.

We have $f \in B \Rightarrow LT(f), LM(f) \in \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I)$, thus $LT(f) \notin LT(I)$ and $LM(f) \in LM(I)$ (**). On the other hand, we have: $f \in A \oplus C \Rightarrow LT(f) \in LT(I)$ or $LM(f) \in NonLM(I)$, which contradicts (**). Hence $B \cap (A \oplus C) = 0$.

(c) Suppose that $f \in C \cap (A \oplus B)$ and $f \neq 0$.

We have $f \in C = \langle\langle NonLM(I) \rangle\rangle \Rightarrow LM(f) \in NonLM(I) \Rightarrow LM(f) \notin LM(I)$ (***). On the other hand, we have $f \in A \oplus B \Rightarrow LM(f) \in LM(I)$ or $LM(f) \in \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I)$ (thus $LM(f) \in LM(I)$), which is contradicts (***). Hence $C \cap (A \oplus B) = 0$.

(2) Now, let us show that $R = A \oplus B \oplus C = I \oplus \langle\langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle\rangle \oplus \langle\langle NonLM(I) \rangle\rangle$.

Suppose that there exists $v \in R$ such that $v \notin A \oplus B \oplus C$ and let us prove that this fact is impossible. Define the set $H = \{LM(v) / v \notin A \oplus B \oplus C\}$, then $H \neq \emptyset$. Let v_0 be a minimal element with the property $LM(v_0) \in H$.

(a) Suppose that $LT(v_0) \in C = \langle\langle NonLM(I) \rangle\rangle$. Let $v_1 = v_0 - LT(v_0)$ then we have $LM(v_1) < LM(v_0)$ (a*). By minimality from (a*), we have $v_1 \in A \oplus B \oplus C$ and $v_0 = v_1 + LT(v_0) \in A \oplus B \oplus C$. Which is impossible by definition of v_0 .

(b) Suppose that $LT(v_0) \notin C = \langle\langle NonLM(I) \rangle\rangle$.

We have $LT(v_0) \notin C = \langle\langle NonLM(I) \rangle\rangle \Rightarrow LM(v_0) \notin NonLM(I)$, thus $LM(v_0) \in LM(I)$, therefore $LT(v_0) \in \mathcal{V}.LM(I)$.

- Suppose that $LT(v_0) \in \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I)$. Let $v_2 = v_0 - LT(v_0) \Rightarrow LM(v_2) < LM(v_0)$ (b*). By minimality from (b*), we have $v_2 \in A \oplus B \oplus C$ and $v_0 = v_2 + LT(v_0) \in A \oplus B \oplus C$, which is impossible.

- Suppose that $LT(v_0) \in \mathcal{V}.LT(I)$, we deduce that there exists $w \in I$ such that $LT(v_0) = LT(w)$. Let $v_3 = v_0 - w \Rightarrow LM(v_3) < LM(v_0)$ (c*). By minimality from (c*), we have $v_3 \in A \oplus B \oplus C$ and $v_0 = v_3 + w \in A \oplus B \oplus C$, which is impossible.

We conclude that $R = A \oplus B \oplus C = I \oplus \langle\langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle\rangle \oplus \langle\langle NonLM(I) \rangle\rangle$ as desired. □

Remark 2.4. - Every element $f \in R$ has a unique decomposition $f = f_1 + \mathcal{N}_I(f)$ where $f_1 \in I$ and $\mathcal{N}_I(f) = f_2 + f_3 \in \langle\langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle\rangle \oplus \langle\langle NonLM(I) \rangle\rangle$. $\mathcal{N}_I(f)$ is called the normal form of f relatively to I .

- Now, a question arise: how to compute the normal form of a polynomial?

As in the commutative case, we are going to see that division by a set of generator of the ideal I

does not solve the problem in general, but division by a noncommutative Gröbner basis of the ideal I solves the problem over a suitable ring.

2.2. Division algorithm.

Division algorithm is already known in the non commutative case over a field [?]. In the following we adapt this algorithm over a ring.

Let $f \in R$, given an ordered set $F = \{f_1, \dots, f_s\} \subset R$, we propose a method to divide f by F i.e. we find nonnegative integers t_1, \dots, t_s and $u_{ij}, v_{ij}, r \in R$ for $1 \leq i \leq s$ and $1 \leq j \leq t_i$ such that:

- (1) $f = \sum_{i=1}^s \sum_{j=1}^{t_i} u_{ij} f_i v_{ij} + r.$
- (2) $LM(f) \geq LM(u_{ij} f_i v_{ij})$ for all i and j .
- (3) $LT(f_i)$ does not divides any term occurring in r for $1 \leq i \leq s$. We will call r a remainder of the division by F .

Algorithm1

INPUT: $F = \{f_1, \dots, f_s\}$ (Ordered), f and an admissible order $<$.

OUTPUT: $t_1, \dots, t_s \in \mathbb{N}, u_{it_i}, v_{it_i}, r \in R$ such that $f = \sum_{i=1}^s \sum_{j=1}^{t_i} u_{ij} f_i v_{ij} + r$

INITIALIZATION: $t_1 = \dots = t_s = 0$, $u_{it_i} = v_{it_i} = r = \emptyset$ and $h := f$.

Divoccur:= False

WHILE $h \neq 0$ and Divoccur:=false **Do**,

IF $LT(f_i)/LT(h)$ (with $LM(h) = u.LM(f_i).v$ and $LC(f_i)/LC(h)$ for $1 \leq i \leq s$ and $u, v \in \mathbb{M}$),
then

$u_{it_i} := [\frac{LC(h)}{LC(f_i)}]u$

$v_{it_i} := v$

DIVOCUR:=True

$h := h - u_{it_i}.f_i.v_{it_i}$

IF DIVOCUR := False, then

$r := r + LT(h)$

$h := h - LT(h)$

Example 2.5. Let $(\mathbb{Z}/16\mathbb{Z})\langle x, y \rangle$. Let us divide $f = 4(xy)^2 - 2xy$ by $f_1 = 3yxy + x^2$ and $f_2 = 2yx - 6y$ with $x >_{\text{grlex}} y$. Then $f = -4x.f_1 + 4x^3 - 2xy$.

- If we start the division by f_2 we get $f = 2x.f_2.y + 12xy^2 - 2xy$.

- If we start the division by f_1 we get $f = -4x.f_1 + 4x^3 - 2xy$

Example 2.6. Let $R = \mathbb{Z}\langle x, y, z \rangle$ and $I = \langle f_1 = 5xy - x, f_2 = 3x^2 - xz \rangle$ be an ideal of R generated by $F = \{f_1, f_2\}$. Let $f = 30zx^2yx \in R$ and $>$ be the (left) graded-lexicographic order on \mathbb{M} with $x > y > z$. The division of f by F yields

- $f = 10z.f_2.yx + 10zxzyx$ if we start by f_2 ,

- $f = 6zx.f_1.x + 2z.f_2.x + 2(zx)^2$ if we start by f_2 .

Notation

If $F = \{g_1, \dots, g_n\}$ is an ordered set in R and $f \in R$, we denote by $r = \overline{f}^F$ a remainder of f under the division by F .

Note that from the above examples, we see that:

-The result of the division algorithm depend on the order on F ,

-The division algorithm doesn't allow to answer the "ideal memberships problem" because if the remainder of the division f by F is r , we doesn't know if $r = \mathcal{N}_I(f)$ is the normal form of f .

In order to solve this two important problems, one must make the division by a noncommutative Gröbner basis as we will see in the following theorem.

Theorem 2.7. Suppose that G is a noncommutative Gröbner basis of an ideal I of R . Let $f \in R$ and assume that $F = \{g_1, \dots, g_n\} = \{g \in G / LM(g) \leq LM(f)\}$. If $\bar{f}^F = r$ ($r \neq 0$) then r is independent of the order of g_1, \dots, g_n in F . In fact $r = \mathcal{N}_I(f)$.

Proof Consider that $\bar{f}^F = r$ ($r \neq 0$), then $LM(r) \leq LM(f)$, since $\langle LT(G) \rangle = \langle LT(I) \rangle$, we see that, for each $g \in G$, $LT(g)$ does not divide any term occurring in r . Hence $r \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle \oplus \langle \langle NonLM(I) \rangle \rangle$. On the other hand, $f = \sum_{i=1}^n \sum_{j=1}^{t_i} u_{ij} g_i v_{ij} + r$ (From the division algorithm) with $LT(g_i)$, $\forall 1 \leq i \leq n$ does not divide any term occurring in r . It is clear that $\sum_{i=1}^n \sum_{j=1}^{t_i} u_{ij} g_i v_{ij} \in I$ and $r \notin I$, that implies $r \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle \oplus \langle \langle NonLM(I) \rangle \rangle$ since the decomposition is unique, we have $r = \mathcal{N}_I(f)$. □

Corollary 2.8. (Ideal membership problem) Suppose that G is a noncommutative Gröbner basis of an ideal I of R . Let $f \in R$, then $f \in I$ if and only if $\bar{f}^G = 0$.

Proof Follows from the above proposition and the fundamental theorem on normal forms. □

2.3. Reduced noncommutative Gröbner basis. Let f be an ideal, a set of term N is a minimal generating set of term if $N = \{ap \in B_J / \forall bq \in B_J, (bq/ap \Rightarrow p = q \text{ and } \langle a \rangle = \langle b \rangle)\}$

Definition 2.9. Let I be an ideal of R and assume that the term-ideal $\langle LT(I) \rangle$ has a unique minimal terms generating set T . We say that the set $G_{I,T}$ is the reduced noncommutative Gröbner basis for I if $G_{I,T} = \{t - \mathcal{N}_I(t)/t \in T \text{ and } \mathcal{N}_I(t) \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle \oplus \langle \langle NonLM(I) \rangle \rangle\}$.

Remark 2.10. The fact of having a unique minimal generating set of terms will guarantee the existence of the reduced noncommutative Gröbner basis.

Theorem 2.11. Let I be an ideal of R and assume that the term-ideal $\langle LT(I) \rangle$ has a unique minimal generating set of terms T_I . Let $G_{I,T}$ be the reduced noncommutative Gröbner basis for the ideal I of R . Then the following hold.

- (1) $G_{I,T}$ is a noncommutative Gröbner basis for I .
- (2) If $g \in G_{I,T}$, then $LC(g) = 1$ or $LC(g) \in \mathcal{V} \setminus \mathcal{V}^*$ is irreducible.
- (3) If $g \in G_{I,T}$ then $g - LT(g) \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle \oplus \langle \langle NonLM(I) \rangle \rangle$.
- (4) $LT(G_{I,T})$ is the minimal terms generating set of $\langle LT(I) \rangle$.

Proof

- (1) $G_{I,T}$ is a noncommutative Gröbner basis for I ?

We have to show that $\langle LT(G_{I,T}) \rangle = \langle LT(I) \rangle$. It is obvious that $G_{I,T} \subseteq I$ and thus $LT(G_{I,T}) \subseteq LT(I)$. Let $f \in I \Rightarrow LT(f) \in LT(I) \subset \langle LT(I) \rangle = \langle T \rangle$, then there exists $t \in T$ such that $t/LT(f)$ (a). Put $g = t - \mathcal{N}_I(t)$ then $LT(g) \in LT(I)$. Recall that $\mathcal{N}_I(t) = t_2 + t_3$ with $t_2 \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle$ and $t_3 \in \langle \langle NonLM(I) \rangle \rangle$ and $g = t - t_2 - t_3$. Since $LT(g) \in LT(I)$ then $LT(g) = LT(t_2)$ or $LT(g) = LT(t_3)$ are impossible, then $LT(g) = t$. Therefore, from (a), we have $LT(g)/LT(f) \Rightarrow LT(f) \in \langle LT(G_{I,T}) \rangle$, thus $\langle LT(I) \rangle = \langle LT(G_{I,T}) \rangle$. Hence $G_{I,T}$ is a noncommutative Gröbner basis for I .

- (2) Obvious.

- (3) If $g \in G_{I,T}$ then $g - LT(g) \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle \oplus \langle \langle NonLM(I) \rangle \rangle$?

Let $g \in G$ then $g = t - \mathcal{N}_I(t)$ (a). From above (1) we have seen that $\mathcal{N}_I(t) \neq LT(g)$ and $LT(g) = t$ (b). Thus from (a) - (b) we find $g - LT(g) = -\mathcal{N}_I(t) \in \langle \langle \mathcal{V}.LM(I) \setminus \mathcal{V}.LT(I) \rangle \rangle \oplus \langle \langle NonLM(I) \rangle \rangle$ as desired.

- (4) $LT(G)$ is the minimal generating set of terms of $\langle LT(I) \rangle$?

Since G is a noncommutative Gröbner basis for I , we have $T \subset LT(G_{I,T})$ as in the above remark. Let $g \in G_{I,T}$ then $g = t - \mathcal{N}_I(t)$, from (2) we have seen that $LT(g) = t \in T \Rightarrow LT(G_{I,T}) \subseteq T$. Thus $T = LT(G_{I,T})$ is the minimal generating set of term of $\langle LT(I) \rangle$. \square

Remark 2.12. *The above theorem guaranties the existence of reduced Gröbner basis but doesn't provide a procedure to compute it, since, until now, we are not able to compute the normal form of a polynomial. In the next section, we will have the necessary tools to compute the normal form of a polynomial.*

3. NONCOMMUTATIVE GRÖBNER BASES OVER NÖETHERIAN VALUATION RING

In this section we will give a way to construct a finite and an infinite noncommutative Gröbner basis by using the overlap relations which generalize S-polynomials for the commutative Gröbner bases [8]. We will also recall the definition of Gröbner basis in the noncommutative case over a field (see: [?]) and adapt it for a valuation ring.

The previous theorem prove that noncommutative Gröbner bases allows to solve the "Ideal membership problem". But, how to compute a Gröbner basis? For this, we need Buchberger's Algorithm.

In this section $R = \mathcal{V}\langle x_1, \dots, x_n \rangle$ is a free associative algebra with non-commuting variables over a commutative ring \mathcal{V} and $<$ an admissible order on the set of all monomials \mathbb{M} .

Minimal generating sets of terms over nœtherian ring

Proposition 3.1. *Let \mathcal{V} be a nœtherian ring and $R = \mathcal{V}\langle x_1 \dots x_n \rangle$. Let \leq be an admissible order on \mathbb{M} . If $J \subset R$ is a term-ideal of R , then J has a unique minimal generating set of terms which is $N = \{ap \in B_J / \forall bq \in B_J, (bq/ap \Rightarrow p = q \text{ and } \langle a \rangle = \langle b \rangle)\}$, where B_J is the set of all terms in J and $\langle \lambda \rangle$ is the ideal of \mathcal{V} generated by $\lambda \in \mathcal{V}$.*

Proof Let S be the set of terms which generates J , i.e $J = \langle S \rangle$. Let $N = \{ap \in B_J / \forall bq \in B_J, (bq/ap \Rightarrow p = q \text{ and } \langle a \rangle = \langle b \rangle)\}$, where $\langle \lambda \rangle$ is the ideal of \mathcal{V} generated by $\lambda \in \mathcal{V}$.

(1) Let us prove that N is nonempty.

Put $\Sigma = \{p \in \mathbb{M} / \exists a \in \mathcal{V}, ap \in S\}$, since \leq is an admissible order on \mathbb{M} , then Σ has a minimal element r .

- If $r \in J$ then $r \in B$, hence $r \in N$ thus N is nonempty.

- If $r \notin J$ then there exists $a \in \mathcal{V} \setminus \mathcal{V}^*$ (i.e a is non-invertible) such that $ar \in S$ because $r \in \Sigma$. Thus, $C_J = \{\langle c \rangle, c \in \mathcal{V} \setminus \mathcal{V}^* / cr \in S\} \neq \emptyset$. Let $\langle c_0 \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \dots \subset \langle c_n \rangle \subset \langle c_{n+1} \rangle \subset \dots$ be an ascending chain of elements of C_J since \mathcal{V} is a nœtherian ring then this chain is stationary i.e there exists c_{i_0} , such that $c_{i_0} = c_i$ for every $i \geq i_0$. Therefore $c_{i_0}r$ is a minimal element and then $c_{i_0}r$ belong to N i.e N is nonempty.

(2) Let us prove that N generates J

Suppose that there exists $ap \in J$ such that $ap \notin \langle N \rangle$; by minimality there exists $bq \notin N$ such that bq/ap and $(p \neq q \text{ or } \langle a \rangle \neq \langle b \rangle)$. But $bq/ap \Rightarrow (q \leq p \text{ or } b/a) \Rightarrow (q \leq p \text{ or } \langle a \rangle \subseteq \langle b \rangle)$ hence using the fact that $p \neq q$ or $\langle a \rangle \neq \langle b \rangle$ we have:

$$ap \notin \langle N \rangle \Rightarrow \exists bq \notin N \text{ such that } q < p \text{ or } \langle a \rangle \subsetneq \langle b \rangle.$$

Now starting by $a_1p_1 \notin \langle N \rangle$ and applying the above result recursively we have an infinite sequence of element $a_i p_i \notin \langle N \rangle$ such that

$$\dots / a_i p_i / \dots / a_2 p_2 / a_1 p_1$$

and at least one of the sequence

$$\dots \leq p_i \leq \dots p_2 \leq p_1 \quad (S_1)$$

and

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots \subseteq \langle a_i \rangle \subseteq \dots \quad (S_2)$$

is infinite.

But the sequence (S_1) is infinite, is impossible because \leq is an admissible order, and also the sequence (S_2) is infinite, is impossible because \mathcal{V} is noetherian.

We can conclude that $\forall ap \in B, ap \in \langle N \rangle$. Thus N is a term generator set of J .

(3) Finally let us prove that N is minimal Suppose that there exist another generating set N' of J such that $N' \subset N$. If $a_0 n_0 \in N, a_0 n_0 \in J = \langle N' \rangle$ then there exists $a' n' \in N'$ such that $a' n'$ divides $a_0 n_0$ and by definition of N we have $\langle a_0 \rangle = \langle a' \rangle$ and $n_0 = n'$ thus $a_0 n_0 = \alpha' a' n' \in N'$ with $\alpha' \in \mathcal{V}$. Hence $N = N'$. \square

Example 3.2. Let consider $<_{grlex}$ order and Let $I \subset R$ be an ideal of R such that

$$I = \langle 2xy^2, 5x^2y, 3x^2, 4yx^2y, 3xy^2, 25xy^2, 25x^2y, 75x^2, 75y^2, 10x^2, 375y^2 \rangle$$

- (1) over $R = \frac{\mathbb{Z}}{5^4\mathbb{Z}}\langle x, y \rangle$, the unique minimal generating set of terms is $N = \{xy^2, x^2, 75y^2\}$.
- (2) over $R = \mathbb{Z}\langle x, y \rangle$, the unique minimal generating set of terms is

$$N = \{3x^2, 10x^2, 75y^2, 2xy^2, 3xy^2, 25xy^2, 5x^2y, 4yx^2y\}$$

Remark 3.3. • The unique minimal generating set of terms given in the above proposition is independent of any particular admissible order.

- The unique minimal generating set of terms is not necessary finite, this differs from the commutative case with Dickson Lemma. For example the ideal $J = \langle xy^i x, i \in \mathbb{N}, i > 1 \rangle$ has an infinite minimal generating set of terms.

Buchberger's Algorithm over a valuation noetherian ring.

First, let us generalize the well known technic of overlap relation for non-commuting multivariate polynomials over a field.

Definition 3.4. (Overlap relation) Let $f, g \in R = \mathcal{V}\langle X_1, \dots, X_n \rangle$ where \mathcal{V} is a valuation ring and R a free associative algebra with n non-commuting variables. Let $<$ be an admissible order on \mathbb{M} . Suppose that there are two monomials p and q :

- (1) $LM(f).p = q.LM(g)$
- (2) $LM(f)$ does not divide q and $LM(g)$ does not divide p .

Then the overlap relation of f and g by p and q is given by:

- $O(f, g, p, q) = \frac{LC(g)}{LC(f)} \cdot f \cdot p - q \cdot g$ if $LC(f)/LC(g)$.
- $O(f, g, p, q) = f \cdot p - \frac{LC(f)}{LC(g)} \cdot q \cdot g$ if $LC(g)/LC(f)$.

Definition 3.5. A subset $D \subset R$ is said to be LM-reduced if for all distinct elements $f, g \in D$, $LM(f)$ does not divide $LM(g)$ and vice versa.

NB: Over a field, every generators set can be LM-reduced in a new generators set, but that is not the case for a valuation ring (see [10]).

We present now the noncommutative version of Buchberger's algorithm over a valuation ring. We began by "Termination Theorem" which is a generalization of Bergman Diamond Lemma ([2], [?]).

Theorem 3.6. Let \mathcal{V} be a noetherian valuation ring and $R = \mathcal{V}\langle x_1, \dots, x_n \rangle$ Suppose that G is a set of LM-reduced elements of $\mathcal{V}\langle x_1, \dots, x_n \rangle$ such that every overlap relation $\overline{O(g, g', p, q)}^G = 0$ with $g, g' \in G$, then G is a noncommutative Gröbner basis for the ideal $I = \langle G \rangle$.

Proof This proof is an adaptation to noetherian valuation ring of the proof in appendix of [?]. Since there are some minor errors:

- in the proof in [?] page 49, for noncommutative Gröbner bases over field,

- and in the computation of S-polynomial of a single polynomial in [25] for commutative Gröbner bases over a valuation ring, (see corrigendum [26]),

we give our proof for the sake of completeness. Let $f \in I$ and assume that $LT(f)$ is not divisible by $LT(g)$ for any $g \in G$. We need to show that this fact is impossible.

Assuming that G is a generating set for I , we have

$$f = \sum_{i,j} \alpha_{ij} p_{ij} g_i q_{ij} = \sum_{i,j} \alpha_{ij} p_{ij} LT(g_i) q_{ij} + \alpha_{ij} p_{ij} [g_i - LT(g_i)] q_{ij} \quad (\Lambda)$$

with $g_i \in G$, p_{ij} , $q_{ij} \in \mathbb{M}$ and $\alpha_{ij} \in \mathcal{V} \setminus \{0\}$. Remark that $LM[p_{ij} LT(g_i) q_{ij}] = p_{ij} LM(g_i) q_{ij}$ and $LM[p_{ij} LT(g_i) q_{ij}] > LM[p_{ij} (g_i - LT(g_i)) q_{ij}]$ for each (i, j) . Let $K = \bigcup_{(i,j)/\alpha_{ij} \neq 0} \{p_{ij} LM(g_i) q_{ij}\}$, $m = \#K$ and write $K = \{p_{i_0 j_0} LM(g_{i_0}) q_{i_0 j_0}, p_{i_1 j_1} LM(g_{i_1}) q_{i_1 j_1} \dots, p_{i_m j_m} LM(g_{i_m}) q_{i_m j_m}\}$ with $p_{i_l j_l} LM(g_{i_l}) q_{i_l j_l} > p_{i_{l+1} j_{l+1}} LM(g_{i_{l+1}}) q_{i_{l+1} j_{l+1}}$, $0 \leq l \leq m-1$.

Let $C_l = \sum_{(i,j)/p_{ij} LM(g_i) q_{ij} = p_{i_l j_l} LM(g_{i_l}) q_{i_l j_l}} LC(g_i) \alpha_{ij}$ and

$$\Gamma_l = \{(i, j) / p_{ij} LM(g_i) q_{ij} = p_{i_l j_l} LM(g_{i_l}) q_{i_l j_l}\}.$$

Since \mathcal{V} is a valuation ring, there exists one of the $LC(g_i)$ occurring in C_l which divides all the others and we denote it by $LC(g_{i(l)})$ and by $p_{i(l)j(l)} LM(g_{i(l)}) q_{i(l)j(l)}$ the corresponding monomial [note that necessarily $p_{i(l)j(l)} LM(g_{i(l)}) q_{i(l)j(l)} = p_{i_l j_l} LM(g_{i_l}) q_{i_l j_l}$ and $LC(g_{i(l)})$ divides C_l , but it is possible to have $LM(g_{i(l)}) \neq LM(g_{i_l})$].

If $C_0 \neq 0$ then necessary

$$LT(f) = C_0 p_{i_0 j_0} LM(g_{i_0}) q_{i_0 j_0} = \frac{C_0}{LC(g_{i(0)})} LC(g_{i(0)}) p_{i(0)j(0)} LM(g_{i(0)}) q_{i(0)j(0)}, \text{ thus}$$

$LT(g_{i(0)}) = LC(g_{i(0)}) LM(g_{i(0)}) / LT(f)$ which contradicts the hypothesis on $LT(f)$. Hence $C_0 = 0$ which implies that $\#\Gamma_0 \geq 2$. Put $z = \max \{l / 0 \leq l \leq m-1, \#\Gamma_l \geq 2\}$, and considering all ways of rewriting f as in (Λ) , we put Γ to be the Γ_z with the smallest size. Let p^* the monomial corresponding to Γ then $\#\Gamma$ is the number of occurrences of p^* in (Λ) . We see that, if we consider all ways of rewriting f as in (Λ) then p^* is the monomial which has the minimal number of occurrences. Therefore, there exists $p, q, p', q' \in \mathbb{M}$ and $g, g' \in G$ such that

$$p^* = p LM(g) q = p' LM(g') q'$$

Now, let us study all possible cases.

Case:1 Suppose that $p < p'$

Case:1.1 Suppose that $q \leq q'$ this forces that $LM(g')$ to divide $LM(g)$, which contradicts the fact that G is LM-reduced.

Case:1.2 Suppose that $q > q'$.

From $p < p'$ and $q < q'$ we can write $p' = p\sigma$ and $q = \rho q'$ (with $\rho, \sigma \in \mathcal{M}$) and using that fact that $p LM(g) q = p' LM(g') q'$, we find $LM(g) \rho = \sigma LM(g')$.

Case:1.2.1 Suppose that $LM(g)$ does not divide σ and $LM(g')$ does not divide ρ . Then there is an overlap of $LM(g)$ and $LM(g')$ from p^* . The corresponding overlap is :

- $O(g, g', \rho, \sigma) = \frac{LC(g')}{LC(g)} \cdot g \cdot \rho - \sigma \cdot g'$ if $LC(g)/LC(g')$,
- and $O(g, g', \rho, \sigma) = g \cdot \rho - \frac{LC(g)}{LC(g')} \cdot \sigma \cdot g'$ if $LC(g')/LC(g)$.

Therefore, we have:

- $p' g' q' = \frac{LC(g')}{LC(g)} p g q - p \cdot O(g, g', \rho, \sigma) q'$ if $LC(g)/LC(g')$,
- and $p g q = p \cdot O(g, g', \rho, \sigma) q' + \frac{LC(g)}{LC(g')} p' g' q'$ if $LC(g')/LC(g)$.

By assumption, $\overline{O(g, g', \rho, \sigma)}^G = 0$, thus we have $O(g, g', \rho, \sigma) = \sum_i \hat{\alpha}_i \hat{p}_i \hat{g}_i \hat{q}_i$ with $\hat{\alpha}_i \in \mathcal{V} \setminus \{0\}$, $\hat{p}_i, \hat{q}_i \in \mathbb{M}$ and $\hat{g}_i \in G$, such that $LM(\hat{p}_i \hat{g}_i \hat{q}_i) < LM(g) \rho = \sigma LM(g')$.

Since $LT(LC(g') p g q) = LC(g') LC(g) p^* = LT(LC(g) p' g' q')$, rewriting $p g q$ and $p' g' q'$ in this way, we can combine their leading term in order to lower the number of occurrences of p^* , which contradicts the minimality of occurrences of p^* .

Case:1.2.2 Suppose that $LM(g)$ divides σ or $LM(g')$ divides ρ , then from $LM(g)\rho = \sigma LM(g')$ we see that $LM(g)$ divides σ and $LM(g')$ divides ρ (hence there is no overlap of g and g' in p^* and $p' > pLM(g)$ and $q > LM(g')q'$).

Now, write $g = \sum_i \alpha_i p_i + LT(g)$ and $g' = \sum_j \alpha'_j p'_j + LT(g')$. We have:

- $\frac{LC(g')}{LC(g)} \cdot pgq - p'g'q' = \frac{LC(g')}{LC(g)} \sum_i \alpha_i pp_iq - \sum_j \alpha'_j p'p'_jq'$ if $LC(g)/LC(g')$,
- and $pgq - \frac{LC(g)}{LC(g')} \cdot p'g'q' = \sum_i \alpha_i pp_iq - \frac{LC(g)}{LC(g')} \sum_j \alpha'_j p'p'_jq'$ if $LC(g')/LC(g)$.

This implies that:

- $p'g'q' = \frac{LC(g')}{LC(g)} pgq - \frac{LC(g')}{LC(g)} \sum_i \alpha_i pp_iq + \sum_j \alpha'_j p'p'_jq'$ if $LC(g)/LC(g')$,
- and $pgq = \sum_i \alpha_i pp_iq - \frac{LC(g)}{LC(g')} \sum_j \alpha'_j p'p'_jq' + \frac{LC(g)}{LC(g')} \cdot p'g'q'$ if $LC(g')/LC(g)$.

We deduce from the previous formulas that rewriting pgq and $p'g'q'$ in this way, we can combine their leading term in order to lower the number of occurrences of p^* , which contradicts the minimality of occurrences of p^* .

Case:2 Suppose that $p = p'$ and we deduce from p^* that $LM(g)q = LM(g')q'$ thus $LM(g)/LM(g')$ or $LM(g')/LM(g)$; which contradicts the fact G is LM-reduced

Case:3 Suppose that $p > p'$: this case is similarly to Case1, by symmetry.

□

We are now ready to give the method to construct a noncommutative Gröbner basis. The procedure is the same than the commutative version, the difference is when computing the overlap relation of two polynomials. Note that in the noncommutative case, the noncommutative Gröbner bases is not necessary finite.

Let \mathcal{V} be a noetherian valuation ring and $R = \mathcal{V}\langle x_1, \dots, x_n \rangle$ a free associative algebra over \mathcal{V} .

Given $f_1, f_2, \dots, f_k \in R = \mathcal{V}\langle x_1, \dots, x_n \rangle$, let $I = \langle f_1, \dots, f_k \rangle$ be a finitely, the algorithm produces a sequence of elements g_1, g_2, \dots , where $g_i = f_i$ for

$1 \leq i \leq k$, and for $i > k$, $g_i \in I$ such that $LT(g_i) \notin \langle LT(g_1), \dots, LT(g_{i-1}) \rangle$.

Algorithm 2

- Input: $\{f_1, f_2, \dots, f_k\}$ a set of LM-reduced elements,
 - Output: $\{g_1, g_2, \dots, g_k, \dots\}$ a noncommutative Gröbner basis for $I = \langle f_1, \dots, f_k \rangle$ for the admissible order
- for $1 \leq i \leq k$, do
 $g_i := f_i$
 $G := \{g_1, \dots, g_k\}$
 Count: k
 Do
 $\mathcal{H} := G$
 For each pair of elements $h, h' \in \mathcal{H}$ and each overlap relation of h, h' ,
 Do
 If $\overline{O(h, h', p, q)}^{\mathcal{H}} = r$ and $r \neq 0$, do
 Count:= count+1
 $g_{count} = r$
 $G := G \cup \{g_{count}\}$
 While $G \neq \mathcal{H}$
 G is a noncommutative Gröbner basis for $I = \langle f_1, \dots, f_k \rangle$ for the admissible order.

Proof: See the above theorem.

Proposition 3.7. *If the terms ideal of I has a finite set of monomial generators, then the above algorithm terminates in a finite numbers of steps and yields a finite Gröbner basis.*

Proof: Similar to the proof of [?] page 21. This case is similarly to the case of noncommutative Gröbner basis over a field and the fact that the ring is a nöetherian valuation ring guaranties that this algorithm terminates.

Example 3.8. Let $f = 3xyx - 2xy$ be a polynomial in $(\mathbb{Z}/4\mathbb{Z})\langle x, y \rangle$ with noncommuting variables. Consider the left graded-lexicographic order with $x > y$ and let us construct a Gröbner basis for the ideal $I = \langle f \rangle$ of $(\mathbb{Z}/4\mathbb{Z})\langle x, y \rangle$. Set $G = \{f\}$, we can easily see that $LM(f) = xyx$ and $LM(f).yx = xy.LM(f)$

then $O_1 = O(f, yx, xy) = 2(xy)^2 - 2xy^2x \rightarrow_f -2xy^2x = f_1$, we replace the previous G by $G = \{f, f_1\}$.

Since $LM(f).y^2x = xy.LM(f_1)$ then $O_2 = O(f, f_1, y^2x, xy) = 0$.

Since $LM(f_1).yx = xy^2.LM(f)$ then $O_3 = O(f_1, f, yx, xy^2) = 0$.

Since $LM(f_1).y^2x = xy^2.LM(f_1)$ then $O_4 = O(f_1, y^2x, xy^2) = 0$.

Hence $G = \{3xyx - 2xy, -2xy^2x\}$ is a Gröbner basis for I in $(\mathbb{Z}/4\mathbb{Z})\langle x, y \rangle$.

Example 3.9. Let $R = \mathbb{Z}/9\mathbb{Z}\langle w, x, y, z \rangle$. Consider the left-graded-lexicographic order with $x > y > z > w$. Let us construct a Gröbner basis for the ideal $I = \langle f_1 = 3yzwx - 2yx, f_2 = 4xy - zw \rangle$ of R . Set $g_1 := f_1, g_2 := f_2$ and $G = \{g_1, g_2\}$. We can easily see that $LM(g_1) = yzwx$, $LM(g_2) = xy$ and $LM(g_1).y = yzw.LM(g_2)$ then $O_1 = O(g_1, g_2, y, yzw) = 3y(zw)^2 - 2yxy \Rightarrow \overline{O(g_1, g_2, y, yzw)}^G = 3y(zw)^2 - 4yzw = g_3$.

The previous G is replaced by $G = \{g_1, g_2, g_3\}$.

Since $LM(g_2).(zw)^2 = x.LM(g_1)$ then $O(g_2, g_1, (zw)^2, x) = -3(zw)^3 - 4xyzw \Rightarrow \overline{O(g_2, g_1, (zw)^2, x)}^G = -3(zw)^3 - 4xyzw = g_4$. The previous G is replaced by $G = \{g_1, g_2, g_3, g_4\}$. Since $\overline{g_3}^{g_4} = 0$, then g_3 is removed from G and the new G is $G = \{g_1, g_2, g_4\}$.

Since there is no more overlap relation in G then G is a Gröbner basis for I in R .

4. NONCOMMUTATIVE GRÖBNER BASES OVER $R = \frac{\mathbb{Z}}{n\mathbb{Z}}\langle x_1, \dots, x_m \rangle$

Let \mathcal{V}_i for $1 \leq i \leq n$ be a finite family of rings such that we are able to compute Noncommutative Gröbner basis G_i in $R_i = \mathcal{V}_i\langle x_1, \dots, x_m \rangle$ which solves the "Ideal membership problem" for $\langle G_i \rangle$, i.e $f_i \in \langle G_i \rangle \Leftrightarrow \overline{f_i}^{G_i} = 0$ for each $1 \leq i \leq k$.

Define the canonical projection $\pi_i : \mathcal{V} = \prod_{j=1}^k \mathcal{V}_j \rightarrow \mathcal{V}_i : a = (a_1, \dots, a_k) \mapsto \pi_i(a) = a_i$. Then

this projection extends naturally in a projection $\pi_i : \prod_{j=1}^k R_j \rightarrow R_i$. If J is an ideal of $\prod_{j=1}^k R_j$ then $J_i = \pi_i(J)$ is an ideal of R_i , and $f \in J \Leftrightarrow f_i = \pi_i(f) \in J_i$ for each $1 \leq i \leq k$. We know that if $J_i = \langle G_i \rangle$, then $f \in J \Leftrightarrow \overline{f_i}^{G_i} = 0, \forall 1 \leq i \leq k$.

Now, since $G = (G_1, \dots, G_k)$ guaranties the "Ideal membership problem" for J , we call G the Dynamical Noncommutative Gröbner basis for J .

If we have a ring isomorphism $\psi : \mathcal{A} \rightarrow \mathcal{V} = \prod_{j=1}^k \mathcal{V}_j$ then it extends naturally in isomorphism $\psi : \mathcal{A}\langle x_1, \dots, x_m \rangle \rightarrow \mathcal{V}\langle x_1, \dots, x_m \rangle$. Now let I be an ideal of $\mathcal{A}\langle x_1, \dots, x_m \rangle$, then $f \in I \Leftrightarrow \psi(f) \in J = \psi(I)$. In this case, we say also that $G = (G_1, \dots, G_k, \psi)$ is the ψ -Dynamical Noncommutative Gröbner basis for I where G_i is a Noncommutative Gröbner basis for $J_i = \pi_i \circ \psi(I)$ for each $1 \leq i \leq k$.

Applications in $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be an integer (where p_k is a prime and $\alpha_j \in \mathbb{N}$) and $\psi : \frac{\mathbb{Z}}{n\mathbb{Z}} \rightarrow \prod_{j=1}^k \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$ be the classical isomorphism from Chinese remainder theorem. Since $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$ is a valuation nöetherian ring, then from section 3, we are able to compute Noncommutative Gröbner bases in $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$.

Therefore, we can solve the "Ideal membership problem" for an ideal in $\frac{\mathbb{Z}}{n\mathbb{Z}}\langle X_1, \dots, X_m \rangle$ by using dynamical process.

Example

Let $n = 24 = 3 \cdot 2^3$ and $I = \langle f_1 = 14xy^2x - 16yx^2, f_2 = 22x^2y^2 - 36yx \rangle$ be the ideal of $\frac{\mathbb{Z}}{24\mathbb{Z}}\langle x, y \rangle$, fix the left graded-lexicographic order with $x > y$. By the Chinese remainder theorem we can define the following isomorphism: $\varphi : \mathbb{Z}/24\mathbb{Z} \rightarrow (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) : x \bmod 24 \mapsto (x \bmod 3, x \bmod 8)$,

Moreover, we have: $\varphi^{-1} : (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) \rightarrow \mathbb{Z}/24\mathbb{Z} : (x \bmod 3, x \bmod 8) \mapsto (16x + 9y) \bmod 24$.

Let us denote by $I_1 = \pi_1(I) = \langle h_1 = 2xy^2x - yx^2, h_2 = x^2y^2 \rangle \subset (\mathbb{Z}/3\mathbb{Z})\langle x, y \rangle$ and $I_2 = \pi_2(I) = \langle h'_1 = 6xy^2x, h'_2 = 6x^2y^2 + 4yx \rangle \subset (\mathbb{Z}/8\mathbb{Z})\langle x, y \rangle$.

We can easily see that $G_1 = \{2xy^2x - yx^2, x^2y^2, xyx^2\}$ is a Gröbner basis for I_1 in $(\mathbb{Z}/3\mathbb{Z})\langle x, y \rangle$ and $G_2 = \{6xy^2x, 6x^2y^2 + 4yx, 4xy^3x, 4yx^2\}$ is a Gröbner basis for I_2 in $(\mathbb{Z}/8\mathbb{Z})\langle x, y \rangle$. Thus $G = \{G_1, G_2, \varphi\}$ is a ψ -dynamical Gröbner basis for I in $(\mathbb{Z}/24\mathbb{Z})\langle x, y \rangle$.

5. NONCOMMUTATIVE GRÖBNER BASES OVER THE INTEGERS

5.1. Special and Dynamical noncommutative Gröbner bases.

Definition 5.1. • S is a multiplicative subset of a ring \mathcal{V} if $S \subseteq \mathcal{V}$, $1 \in S$ and $\forall x, y \in S$, $xy \in S$.

- $\mathcal{M}(x_1, \dots, x_r) = \{x_1^{n_1} \times \dots \times x_r^{n_r}, n_i \in \mathbb{N}\}$ is the multiplicative subset of \mathcal{V} generated by $\{x_1, \dots, x_r\}$ where $x_1, \dots, x_r \in \mathcal{V}$. Briefly, we denote $x^{\mathbb{N}} = \mathcal{M}(x) = \{x^n, n \in \mathbb{N}\}$.
- Let S be a multiplicative subset of a ring \mathcal{V} . The ring $S^{-1}\mathcal{V} = \{\frac{x}{s}, x \in \mathcal{V}; s \in S\}$ is the localization of \mathcal{V} relatively to S .
- Let $x \in \mathcal{V}$, we denote by $\mathcal{V}_{[x]}$, the localization of \mathcal{V} relatively to the multiplicative subset $x^{\mathbb{N}}$. Moreover, one can define by induction $\mathcal{V}_{[x_1, x_2, \dots, x_k]} := (\mathcal{V}_{[x_1, x_2, \dots, x_{k-1}]})_{[x_k]}$ for $x_1, \dots, x_k \in \mathcal{V}$.
- The multiplicative subsets S_1, \dots, S_k of a ring \mathcal{V} are called comaximal if $\forall s_1 \in S_1, \dots, s_n \in S_n; \exists v_1, \dots, v_n \in \mathcal{V}$ such that $\sum_{i=1}^n v_i s_i = 1$.

Definition 5.2. - Let \mathcal{V} be a Principal ideal ring, $f, g \in \mathcal{V}\langle x_1, \dots, x_n \rangle \setminus \{0\}$, $I = \langle f_1, \dots, f_s \rangle$ be a nonzero finitely generated ideal of $\mathcal{V}\langle X_1, \dots, X_n \rangle$, and $>$ an admissible order.

- If $G = \{g_1, \dots, g_t\}$ and $\{LC(g_1), \dots, LC(g_t)\}$ are totally ordered under division then it is possible to define for each (i, j) , the overlap of g_i and g_j such as on valuation rings. Therefore, we are able to generalize noncommutative Gröbner basis to Principal ideal rings.

- For $g_1, \dots, g_t \in \mathcal{V}\langle X_1, \dots, X_n \rangle$, $G = \{g_1, \dots, g_t\}$ is said to be a special noncommutative Gröbner basis for I if $I = \langle g_1, \dots, g_t \rangle$, the set $\{LC(g_1), \dots, LC(g_t)\}$ is totally ordered under division and for each $(g, g') \in G \times G$, $\overline{O(g, g', p, q)}^G = 0$.
- A set $G = \{(S_1, G_1), \dots, (S_k, G_k)\}$ is said to be a dynamical noncommutative Gröbner basis for I if S_1, \dots, S_k are finite comaximal multiplicative subsets of \mathcal{V} and in each localization $(S_i^{-1}\mathcal{V})[X_1, \dots, X_n]$, G_i is a special noncommutative Gröbner basis for $S_i^{-1}I$.

NB If \mathcal{V} be a Principal ideal ring then each localization $S_i^{-1}\mathcal{V}$ is a Principal ideal ring

Proposition 5.3. Let \mathcal{V} be a Principal ideal ring, $I = \langle f_1, \dots, f_s \rangle$ a nonzero finitely-generated ideal of $\mathcal{V}\langle X_1, \dots, X_n \rangle$. Let $f \in \mathcal{V}\langle X_1, \dots, X_n \rangle$ and fix an admissible order. Suppose that $G = \{g_1, \dots, g_t\}$ is a special noncommutative Gröbner basis for I in $\mathcal{V}\langle X_1, \dots, X_n \rangle$. Then, $f \in I$ if and only if $\overline{f}^G = 0$.

Proof Similar to the one of Special commutative Gröbner basis over a Principal ideal ring in [25] and in corrigendum [26]. \square

Theorem 5.4. Let \mathcal{V} be a Principal ideal rings, $I = \langle f_1, \dots, f_s \rangle$ a nonzero finitely-generated ideal of $\mathcal{V}\langle x_1, \dots, x_n \rangle$, $f \in \mathcal{V}\langle x_1, \dots, x_n \rangle$ and fix an admissible order on $\mathcal{V}\langle x_1, \dots, x_n \rangle$. Suppose that $G = \{(S_1, G_1), \dots, (S_k, G_k)\}$ is a dynamical noncommutative Gröbner basis for I in $\mathcal{V}\langle x_1, \dots, x_n \rangle$. Then, $f \in I$ if and only if $\overline{f}^{G_i} = 0$ in $(S_i^{-1}\mathcal{V})[X_1, \dots, X_n]$ for each $1 \leq i \leq k$.

Proof: Similar to the one of Dynamical commutative Gröbner basis over a Principal ideal ring in [25] and in corrigendum [26].

5.2. Buchberger's algorithm for Dynamical noncommutative Gröbner basis. .

We are now ready to present the algorithm to construct a Special and a Dynamical noncommutative Gröbner basis for an ideal $I = \langle f_1, \dots, f_s \rangle$ of $R = \mathbb{Z}\langle X_1, \dots, X_n \rangle$.

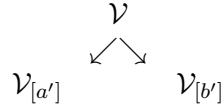
Comparatively to noetherian valuation ring, we can find two incomparable (under division) elements $a, b \in \mathcal{V}$. In this case, one should compute $d = a \wedge b$, factorize $a = da'$, $b = db'$, with $a' \wedge b' = 1$, and then open two branches from \mathcal{V} , the computations are pursued in $\mathcal{V}_{[a']}$ and $\mathcal{V}_{[b]}$.

Case of overlap relation The overlap relation of f and g by p and q is given as follow:

- If $LC(f)$ and $LC(g)$ are comparable in \mathcal{V} under the division order then apply the classical definition (as in a valuation ring);

- If $LC(f)$ and $LC(g)$ are not comparable in \mathcal{V} under the division order then:

- (1) write $LC(f) = (LC(f) \wedge LC(g)).a'$ and $LC(g) = (LC(f) \wedge LC(g)).b'$ where $a' \wedge b' = 1$ and $LC(f) \wedge LC(g) = \gcd(LC(f), LC(g))$ and open two branch:



- (2) in $\mathcal{V}_{[a']} = \{ \frac{c}{a'^n} / c \in \mathcal{V} \text{ and } n \in \mathbb{N} \}$, a' is invertible and $LC(f)$ divides $LC(g)$, then the overlap relation is:

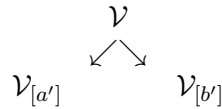
$$O(f, g, p, q) = \frac{LC(g)}{LC(f)} \cdot f \cdot p - q \cdot g.$$

- (3) in $\mathcal{V}_{[b']} = \{ \frac{c}{b'^n} / c \in \mathcal{V} \text{ and } n \in \mathbb{N} \}$, b' is invertible and $LC(g)$ divides $LC(f)$, then the overlap relation is:

$$O(f, g, p, q) = f \cdot p - \frac{LC(f)}{LC(g)} \cdot q \cdot g$$

Case of division algorithm For the division of f by g , if one has to divide $LT(f) = LC(f)LM(f)$ by $LT(g) = LC(g)LM(g)$ with $LM(g)/LM(f)$ and $LC(f)$ and $LC(g)$ are not comparable in \mathcal{V} under the division order then:

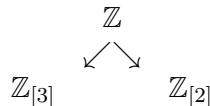
- (1) write $LM(f) = uLM(g)v$ with $u, v \in \mathbb{M}$,
- (2) write $LC(f) = (LC(f) \wedge LC(g)).a'$ and $LC(g) = (LC(f) \wedge LC(g)).b'$ where $a' \wedge b' = 1$ and $LC(f) \wedge LC(g) = \gcd(LC(f), LC(g))$ and open two branch:



- (3) in $\mathcal{V}_{[a']}$: $f = \frac{a'}{b'}u.g.v - r$ and the division is pursue were f will be replaced by r .
- (4) in $\mathcal{V}_{[b]}$: $LT(f)$ is not divisible by $LT(g)$ and therefore $f = \bar{f}^{\{g\}}$

Example 5.5. Overlap relation

Let $f_1 = 6yzwx - 2yx$ and $f_2 = 4xy - 5zw$ be two polynomials in $R = \mathbb{Z}\langle x, y, z, w \rangle$ such that $w < x < y < z$, fix the left graded-lexicographic order. We have: $LM(f_1).y = yzw.LM(f_2)$ and $LC(f_1)$ does not divides $LC(f_2)$ and vice versa, in this case we have: $LC(f_1) = (LC(f_1) \wedge LC(f_2)).a' = (6 \wedge 4).3$ and $LC(f_2) = (LC(f_1) \wedge LC(f_2)).b' = (6 \wedge 4).2$.



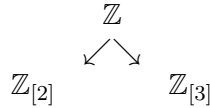
First case: In $\mathbb{Z}_{[3]} = \{\frac{a}{3^n}/a \in \mathbb{Z}, n \in \mathbb{N}\}$, 3 is invertible and $LC(f_1)$ divides $LC(f_2)$ then

$$O(f_1, f_2, y, yzw) = \frac{LC(f_2)}{LC(f_1)} \cdot f_1 \cdot y - (yzw) \cdot f_2 = 5yzwxy - \frac{4}{3}yxy$$

Second case: In $\mathbb{Z}_{[2]} = \{\frac{a}{2^n}/a \in \mathbb{Z}, n \in \mathbb{N}\}$, 2 is invertible and $LC(f_2)$ divides $LC(f_1)$ then

$$O(f_1, f_2, y, yzw) = f_1 \cdot y - \frac{LC(f_1)}{LC(f_2)} \cdot (yzw) \cdot f_2 = \frac{15}{2}y(zw)^2 - 2yxy$$

Example 5.6. Buchberger's algorithm Let $R = \mathbb{Z}\langle x, y \rangle$ be a free associative algebra, $I = \langle f_1 = 6xyx - 8xy, f_2 = 4xy - 3yx \rangle$ be an ideal of R and we fix an admissible order with $x >_{\text{grlex}} y$. Set $G = \{g_1 = 6xyx - 8xy, g_2 = 4xy - 3yx\}$, our goal is to construct a noncommutative Gröbner basis for I in R . We have: $LM(g_1) \cdot yx = xy \cdot LM(g_1)$, then $\overline{O(g_1, yx, xy)}^G = 6yx^2y - y^2x = g_3$ and $G := G \cup \{g_3\} = \{g_1, g_2, g_3\}$. Notice that $LC(g_1) = 6$, $LC(g_2) = 4$ and both are incomparable under division in \mathbb{Z} , then we open from \mathbb{Z} two branches $\mathbb{Z}_{[2]}$ and $\mathbb{Z}_{[3]}$ and pursued the computation of overlap relations in each branch:



- In the ring $\mathbb{Z}_{[2]}$, the set $G_1 = \{6xyx - 8xy, 4xy - 3yx, \frac{-9}{2}yx^2 + 6yx, \frac{3}{2}y^2x\}$ is a Gröbner basis for $(2^{\mathbb{N}})^{-1}I$ in $((2^{\mathbb{N}})^{-1}\mathbb{Z})\langle x, y \rangle$, in the other hand G_1 is a special Gröbner basis for I in R .
- In the ring $\mathbb{Z}_{[3]}$, the set $G_2 = \{6xyx - 8xy, 4xy - 3yx, 3xy^2x - 3y^2x, -3yx^2 + 4yx, -3(yx)^2 + 4y^2x, \frac{64}{3}yx, y^3x, -2y^2x\}$ is a Gröbner basis for $(3^{\mathbb{N}})^{-1}I$ in $((3^{\mathbb{N}})^{-1}\mathbb{Z})\langle x, y \rangle$, in the other hand, G_2 is a special Gröbner basis for I in R .

Thus the set $G = \{(G_1, (2^{\mathbb{N}})), (G_2, (3^{\mathbb{N}}))\}$ is a dynamical Gröbner basis for I in R .

6. ACKNOWLEDGMENT

Author is grateful to the IMU Berlin Einstein Foundation, the Berlin Mathematical School and to Pr.Dr. Klaus Altmann for receiving him in Berlin during the writing of the important part of this paper.

REFERENCES

- [1] D. Augot, J.-C. Faugère, L. P. *Gröbner Bases Techniques in Cryptography and Coding Theory*. Special Issue, Journal of Symbolic Computation, 2010
- [2] G. Bergman, *The diamond lemma for ring theory* Adv Math. 29 (1978), 178-218
- [3] B. Buchberger, *Ein Algorithmus zum Auffinden der basiselemente des Restklassenringes nach einem nulldimensionalen polynomideal*, PhD thesis, University of Innsbruck, Austria, 1965.
- [4] B. Buchberger. *An algorithm for finding a bases for the residue class ring of a zero-dimensional polynomial ideal (in German)*. Ph.D. Thesis, Univ. of Innsbruck, Austria, Math., Inst. 1965
- [5] B. Buchberger *A critical-pair/completion algorithm in reduction rings*. In: (E. Borger, G. Hasenjaeger, D. Rodding, eds.) Proc. Logic and Machines: Decision Problems and Complexity, Springer LNCS 171, 137-161; 1984
- [6] B. Buchberger. *Introduction to Gröbner bases*. In: (B. Buchberger, F. Winkler, eds.) Gröbner bases and Applications, London Mathematical Society Lecture Note Series 251, Cambridge University Press. 1998
- [7] S. Cojocaru, V. Ufnarovski, *Noncommutative Gröbner bases, Hilbert series, Anick's Resolution and BERGMAN under MS-DOS*. Computer Science Journal of Moldova 3 (1995), pp. 24-39.
- [8] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, 3rd ed., Springer-Verlag, New York, 2007.

- [9] J.-C Faugère, L. Perret. *Efficient Computation of Gröbner Bases and Applications in Cryptography*. Springer. 2010
- [10] E. Green, *An introduction to noncommutative Gröbner bases*, In: Fisher K. G.(ed.), Computational Algebra, Dekker, New York.(Lecture Notes in Pure and Applied Mathematics 151): 1998, 167-190.
- [11] E. Green: *Noncommutative Gröbner bases, and projective resolutions. Computational methods for representations of groups and algebras*. Papers from the First Euroconference held at the University of Essen. Basel, 1999, P. Dräxler, G. O. Michler, and C. M. Ringel, Eds., no. 173 in Progress in Math., Birkhäuser Verlag, pp. 29-60.
- [12] E. Green: *Multiplicative bases, Gröbner bases, and right Gröbner bases*. Jour. Symb. Comput., 2000.
- [13] E. Green, L. S. Heath and B. J. Keller: *Opal: A system for computing noncommutative Gröbner bases (system description)*. Eighth International Conference on Rewriting Techniques and Applications (RTA-97), 1997, pp. 331- 334.
- [14] E. Green , T. Mora , V. Ufnarovski , *The Non-Commutative Gröbner Freaks*.Progress in Computer Science and Applied Logic Birkhäuser 15 (1991), pp. 93-104.
- [15] A. H. Kacem, I. Yengui, *Dynamical Gröbner bases over Dedekind rings*, J. Algebra **324** (2010) 12-24.
- [16] D. Kapur and K. Madlener *Construction of Gröbner bases in "special" rings*, in "Manuscript presented at the Gröbner bases workshop 1988", Cornell.
- [17] A. Kandri-Rody and D. Kapur *Computing a Gröbner bases of a polynomial ideal over a Euclidean domain*, J. Symbolic Computation 6, 37-57, 1988.
- [18] A. Kandri-Rody and V. Weispfenning, *Non-commutative Gröbner bases in algebras of solvable type*, J. Symb. Comp. vol.6(2/3): 371-388, 1987.
- [19] F. Mora: *Gröbner bases for non-commutative polynomial rings*. Proc. AAEECC3, LNCS 229. Springer-Verlag, Berlin, New York, 1986.
- [20] T. Mora, *An introduction to commutative and noncommutative Gröbner bases*, Theor. Comp. Sci., 134: 131-173, 1994.
- [21] T. Mora, M. Sala, C. Traverso, L. P., M. Sakata. *Gröbner Bases, Coding, and Cryptography*. RISC book series (Springer, Heidelberg). 2010
- [22] T. S. Rai, *Infinite Gröbner Bases and Noncommutative Polly Cracker Cryptosystems*. Ph.D thesis, Virginia Polytechnic Institute and State University, 2004. <http://scholar.lib.vt.edu/theses/available/etd-03262004-082608/unrestricted/rai-etd.pdf>
- [23] S. Stifter . *A generalization of reduction rings*. J. Symbolic Computation, 4, 351-364. 1987
- [24] S. Stifter *Gröbner bases of modules over reduction rings*. J. Algebra, 159, 54-63. 1993.
- [25] I. Yengui, *Dynamical Gröbner bases*. J. Algebra **301** (2006) 447-458.
- [26] I. Yengui, *Corrigendum to "Dynamical Gröbner bases"* [J. Algebra 301 (2) (2006) 447-458] & to "*Dynamical Gröbner bases over Dedekind rings*" [J. Algebra 324 (1) (2010) 12-24]. Preprint 2010.